NAVAL WAR COLLEGE
Newport, R. I.

LIMITLESS BATTLESPACE:
Operations in Cyberspace

by

Carolyn J. Lee
Civilian, United States Air Force

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Departments of the Navy or Air Force.

Signature: Carolyn J. Lee

17 May 1999

Security Classification This Page Unclassified

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization:
JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol: C

7. Address: NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. Title (Include Security Classification):
LIMITLESS BATTLESPACE: Operations in Cyberspace (Unclassified)

9. Personal Authors: Carolyn J. Lee, CIV

10. Type of Report: FINAL

11. Date of Report: 17 May 1999

12. Page Count: 24

13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy or the Department of the Air Force.

14. Ten key words that relate to your paper: Information operations, cyberspace, operations, IMOC, networks, internet, infrastructure, information power

15. Abstract: Our nation is embarked on a new Cold War. This new war, unlike the conflict with the Soviet Union, has no territorial boundaries, can involve offensive operations from virtually any corner of the globe, can be conducted by nation-states, terrorist groups or high school hackers, and requires massive national expenditure to counter. It is a product of the Information Age. This war in a military context can be undertaken on its own or in concert with traditional employment of force. It can also be a force multiplier both for and against our nation.

In the modern world, the territorial boundaries between adversaries and allies can be unrecognizable as in the case of non-State-sponsored terrorism, space, and cyberspace. For the operational commander, use of information technology including space systems will generally traverse networks within and possibly controlled by nations not involved in the conflict, and over which he has no control. In fact, his information may actually employ the adversary's assets en route to him. Such is the nature of "information operations" in modern society.

As presented here, the advent of this technology presents unique capabilities as well as unique problems and vulnerabilities for military operations. This paper intends to address:

-- The unique nature of cyberspace
-- Potential vulnerabilities to (specifically) command and control systems
-- Measures for information management and protection
-- Challenges of information operations

While this paper does not endorse restricted use of the technology, it will attempt to raise the awareness of the operational commander regarding this new venue of war, and proposes a CINC-level organization to effectively operate in the information realm.

16. Distribution / Availability of Abstract:	Unclassified	Same As Rpt	DTIC Users
	X		

17. Abstract Security Classification: UNCLASSIFIED

18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19. Telephone: 841-6461 **20. Office Symbol:** C

Abstract of

LIMITLESS BATTLESPACE: OPERATIONS IN CYBERSPACE

Our nation is embarked on a new Cold War. This new war, unlike the conflict with the Soviet Union, has no territorial boundaries, can involve offensive operations from virtually any corner of the globe, can be conducted by nation-states, terrorist groups or high school hackers, and requires massive national expenditure to counter. It is a product of the Information Age. At issue is the unique nature of this war, behavior of belligerents, and operational maneuvers available to the commander. This war in a military context can be undertaken on its own or in concert with traditional employment of force. It can also be a force mulitplier both for and against our nation.

In the modern world, the territorial boundaries between adversaries and allies can be unrecognizable as in the case of non-State-sponsored terrorism, space, and cyberspace. For the operational commander, use of information technology including space systems will generally traverse networks within and possibly controlled by nations not involved in the conflict, and over which he has no control. In fact, his information may actually employ the adversary's assets en route to him. Such is the nature of "information operations" in modern society.

As presented here, the advent of this technology presents unique capabilities as well as unique problems and vulnerabilities for military operations. This paper intends to address:

-- The unique nature of cyberspace

-- Potential vulnerabilities to (specifically) command and control systems

-- Measures for information management and protection

-- Challenges of information operations

While this paper does not endorse restricted use of the technology, it will attempt to raise the awareness of the operational commander regarding this new venue of war and proposes a CINC-level organization to effectively operate in the information realm.

TABLE OF CONTENTS

"Information technology and processes, when synthesized by operational art and new organizational concepts, present an opportunity for discontinuous change--a great leap in warfighting--from the industrial to information age."[1]

I. Introduction

Revolutions in information technology have enabled the Department of Defense and associated agencies to provide unprecedented volumes of information to our nation's decision makers as well as the front line warfighters. This capability expands the realm of battle for both the U.S. and our adversaries with potential to actually determine the outcome of war if properly addressed. The networks and systems comprising this "opportunity" must therefore be provided the same threat analysis, protection, and target mitigation as other major weapon systems. This treatment as well as the day to day mission of managing data extracted from an expanding base of sources must be entrenched in military operations if we are to effectively influence the battlespace. Further, industrialized nations including potential enemies spend large percentages of their Gross Domestic Product to acquire, manipulate and protect vital information as a national resource. This international quest is the new Cold War as countries strive to acquire information and technology that will place them ahead of their adversaries both militarily and economically.

The United States military not only links their administrative information via a complex systems network, but advanced intelligence, surveillance and reconnaissance capabilities enable the U.S. to engage around the globe at unprecedented speed. Knowledge gleaned from and processed by these information systems is vital to defense weaponry and military -- indeed national -- maneuvers. Even with this realization, however, there is a

---

[1]Casper et al, "Knowledged-Based Warfare: A Security Strategy for the Next Century," *Joint Forces*

profound reluctance within the Department of Defense (DOD) to elevate this vital element to the level of weapons system. As argued here, we must not only place information systems equal to (perhaps higher than) weapons systems, but we must organize at the CINC level to conduct operations in this information sphere, employ information operators as part of the Joint Task Force (JTF), and teach our leaders the art of operating in the fourth dimension.

This dimension has no territorial boundaries to defend and may have no identifiable opponents to engage. That is, information operations (IO) can take place from any corner of the globe and be the work of recognized nation-states, obscure terrorist groups, or simply high school hackers looking for prestige within their own subculture. Yet information operations are capable of damage comparable to traditional weapons of mass destruction (WMD). When one considers the potential to disrupt power grids, entire telecommunication or air traffic control networks, nuclear plant operations, or environmental containment systems, it's obvious the effects of system interruption (or destruction) are monumental and cascading. Given the ease and low cost to effect this damage, the nation is more at risk of these types of operations than guerilla, conventional or nuclear conflict. Just as in other types of conflict affecting our nation, it is the job of the DOD take actions necessary to mitigate this threat. In this realm, the knowledge system (inclusive of information systems, communication links and databases) are analogous to precision guided munitions and deserve the title of weapons system.

Quarterly, Ft McNair: Washington DC, Autumn 1996, pg 82

II. Terrae Incognita

"Information has become tantamount to space and is in the process of becoming an actual place . . . Cyberspace is assuredly a region--but oddly so, and a troubling and ill-mannered one."[2]

The American history of war has always included the identifiable parameters of territory, cause, and tangible adversary. Against these parameters we have developed armament capable of traversing any terrain, engaging any adversary, for any cause deemed appropriate by our leadership. We trained our forces to maximize the potential of this armament, developed doctrine to synergize their employment and modified tactics as necessary to stay ahead of the opponent. In the twenty-first century, however, we face a new battlespace. Much to the chagrin of the traditionalist military, the new battlefield will involve faceless entities operating within a global information grid and employing little more than a small computer network either stand-alone or in concert with military force. The astute military commander, therefore, must either be comfortable with the precepts of this new region of war or proceed at extreme peril.

Admittedly, cyberspace requires a mental orientation unfamiliar to the operational art of war. A nation's physical, social, cultural, and industrial boundaries can be crossed with no respect to nationality or intentions of the traveler -- it is the ultimate "global village." It has generated a subculture of its own with no real physical center or allegiance to any government. It has even been described as the modern equivalent to the 19th century West:

---

[2]Starrs, Paul F., "The Sacred, the Regional, and the Digital," *Geographical Review*, Vol. 87, New York: Apr. 1997, pg 195

". . . vast, unmapped, culturally and legally ambiguous, verbally terse . . .hard to get around in, and up for grabs."[3]

Understanding this vastness is imperative. As the United States reaches for global engagement capability, the command and control infrastructure necessary to support such ambitions is constantly under pressure. Although the internet has exploded from just four nodes in 1969 to approximately 30 million by January 1998,[4] the technology has not been distributed evenly. In the environments occupying much of our focus today such as Africa and the Middle East, in-place communication systems are generally insufficient to support the high-speed, large data volume requirements associated with deployment of the U.S. military. Hence, the forward commander must be fully cognizant of the information infrastructure available, the potential threats and the means necessary to overcome identified shortfalls. First and foremost, he must determine information priorities. In this context we are not concerned solely with intelligence data, but with those sources and links necessary to conduct his mission on a daily basis (see note i). His requirements may run the gamut from weather reports to generation or receipt of orders to forwarding of logistical requirements or identification of medical evacuations. In addition, he must assume the enemy is capable of impeding his mission through counter information operations and plan a flexible response. Without the ability to communicate freely with echelons of command, receive updated intelligence reports or acquire targeting data for today's smart weapons, the commander has only a myopic view of the battlespace and enemy activities. Nevertheless, just as information systems can be a

---

[3]Ibid, pg 200

[4]Dodge, M., "An Atlas of Cyberspace," *Cyber-Geography Research*, Center for Advanced Spatial Analysis, University College, London (1998) (http://www.cybergeography.org/atlas/atlas.html)

vulnerability, the reverse is also true -- information and information systems can be a significant force multiplier to those using them most efficiently and effectively.

III. Operational Concerns

"A key characteristic of future warfare is an increased operations tempo that stresses a commander's ability to observe and react to changes in the battlespace . . . the commander operating at a faster tempo will always be one step ahead of an adversary and is actually setting the tempo . . . the time differential between [orienting and deciding] has compressed to the point that in information age warfare, orienting and deciding can no longer be sequential actions but must be simultaneous and continuous ones"[5]

The first Secretary of Defense Strategic Studies Group identified Knowledged-based Warfare as "a process that provides superior situation awareness of the battlespace, allowing us to decide at a faster pace than an enemy."[6] Superior knowledge of our opponent enables us to work for discrete effects of war rather than overwhelming destruction. As demonstrated in Desert Storm, Bosnia, and again in Kosovo operations, precision guided munitions directed to key targets are able to achieve maximum destruction to enemy capability without massive collateral civilian casualties. This in turn improves the legitimacy of forcible action in other-than-declared-war conditions, retains public support, and does not cripple the opponent to the extent he must fight for survival (precluding escalation of the conflict).

The psychological effect of overwhelming knowledge can also be a significant deterrent to enemy forces. With comprehensive battlespace awareness, the operational commander is able to detect enemy movements even with the enemy's best attempts at subterfuge. The enemy, in turn, has no place to hide, no means of outmaneuvering his opponent and is in effect totally exposed to the superior information of his opponent (see note

---

[5]Roman, Gregory A. "The Command or Control Dilemma: When Technology and Organizational Orientation Collide," *Essays on Strategy XIV*, National Defense University: Washington DC (March 1997) pg 156
[6]Casper et al, pg 82

ii). This ability to conduct high intensity, parallel, and devastating warfare leaves the enemy no time to rest and recover as in sequential warfare. Further, the combat agility provided through superior battlespace knowledge delivered faster and more reliably to forces enables the commander to control the tempo of the operation.

If we concede that information may very well determine the outcome of any conflict, we can then begin to treat information systems and their capabilities as vital weapons systems requiring the same treatment as other high value weapons systems: threat analysis, protection and damage mitigation.. This opinion was echoed by Lt. Gen Lance Lord, Air Force Space Command Vice Commander, in that Command's Enterprise Network and Information Technology Strategy Letter dated 31 December, 1997, which urged a weapons systems approach to the Air Force's "Enterprise Networks" with corresponding resources and professional management such as one would apply to any mission critical asset.[7]

IV. The Fog of Reality

"Information technology has some effects on the use of force that benefit the small and some that favor the powerful. The off-the-shelf commercial availability of what used to be costly military technologies benefits small states and nonstate actors and increases the vulnerability of large states. Information systems add lucrative targets for terrorist groups."[8]

We have often read of the *fog of war* with some authors promising its dispersal by application of the latest information technology. It is true that the technology revolution currently underway provides the warfighter with improved imagery, greater access to all levels of operational data of both U.S. and foreign forces, and almost instantaneous communication capabilities. An important and necessary caution, however, is that one can not always be sure

[7]As quoted by Megan C. Block, Capt, "AFSPC Develops Info Technology Strategy for 21st Century, *Intercom (Jul. 98):7*

of what is being seen, heard, or transmitted. That is, technology has advanced to such an extent that even the least technologically advanced nation (or high school student) has the capability to alter those data points with minimal chance of detection.

Causing an operator to doubt his information is just as effective a paralysis as overcoming him by force - he is unable to launch his missiles if he can't be sure of the target coordinates, he is not likely to release his fighters if he cannot be sure of the surface-to-air missiles locations and he'll hesitate to move his ships into potentially mine infested waters if he cannot trust the intelligence report stating the coast is clear. It is a remarkable form of psychological operation:

> "Our objective in war or strategy is the behavior of a limited number of people. We wish to conduct our affairs in such a way that these people will act in a way that we prefer--our goal in strategy is to influence human behavior in a way favorable to our objectives. I suggest, then, that our strategies ought to seek this as their principal object--the mind of the opposing commander".[9]

Equally important, we must prevent our opponent from influencing the minds of our own commanders. We must deliver the best possible ground truth garnered from trusted sources and validated to the greatest extent possible given time and resources. Obviously, the higher value data warrants our best protection practices, but no information system organization - military or commercial - can deliver on promises of absolute security. As our methods and procedures to counter network intrusions change, so do the tactics of our etherworld opponents.

---

[8]Keohane, Robert O. and Joseph S. Nye, Jr., "Power and Interdependence in the Information Age," *Foreign Affairs*, Vol. 77, No. 5, New York, NY (Sep./Oct. 1998) pg 88

[9]Lieutenant General Raymond B. Furlong, "Strategymaking for the 1980s," *Parameters, Journal of the US Army War College* 9 (March 1979):10

DOD certainly has not ignored the criticality of information. Several information protection organizations have been established throughout the services and leadership has introduced the concept of "Information Operations" into the military lexicon. However, the majority of attention is applied to protecting our networks. Too often this activity is viewed as a secondary concern by commanders uneducated on the expertise residing within the opposing side (that is, anyone intent on adversely affecting U.S. military operations or capabilities). A corresponding but equally important function is *validation of the data* received, processed, and stored.

V. 21st Century Warfighting: Information Management and Operations

"A plenitude of information leads to a poverty of attention. Attention becomes the scarce resource, and those who can distinguish valuable signals from white noise gain power. Editors, filters, interpreters, and cue-givers become more in demand, and this is a source of power. There will be an imperfect market for evaluators."[10]

Once conceded as a vital part of the warfighting apparatus, the establishment of an information processing/management/warfighting/dissemination center becomes of utmost importance. This integrated process, preferably physically collocated and with redundancy capability, must encompass all aspects of the information realm to include data gathering, validation, correlation, and dissemination. In addition, it must be able to accomplish the transformation of data-to-information-to-knowledge through support of the operational arms of air, land, sea and space warfare using tailored products and knowledge multipliers. In conjunction with daily operations, care must be taken to protect data and communication links from tampering, identify those areas being targeted by hostile forces, and retaliate with counter information technology as deemed appropriate for self preservation or to influence the

[10]Keohane, pg 89

enemy's operations. Above all else, it must be responsive to the warfighting CINC, deployable to an operational area, and employ technical masters of effects based warfare including cyberspace maneuvers.

The theoretical organization presented here includes a core of information systems specialists supporting cells of experienced operators in air, land, sea and special operations warfare. It is the first step in achieving information superiority over the enemy and capitalizing on all data available at the national, regional, operational, and tactical levels. The Information Management and Operations Center (IMOC) would provide five essential services to the operational cells: Information Management, Network Management, Information Intelligence, Strategic Knowledge and Ops/Counter Ops. Each aspect is an integral part in exploiting both the wealth of information available and the latest in information technologies. Nevertheless, when placed together they form the most influential operational force in the DOD's inventory (an opinion sure to raise the ire of traditional "operators").

Information Management

The term "information management" (IM) as used here is not merely the functions of cataloguing, filing, and controlling the data, but expands to data acquisition, validation, and consolidation. The function of this IM is not only receipt of data from DOD and other agency sources, but an active search for similar and related information using all available information technologies. "Information in any form, at any time and from anywhere demands not just technology, but the thoughtful application of technology" states Ken Pedersen (co-

chairperson) during a technical exchange meeting on network-centric computing.[11] This activity is well applied by intelligence agencies, and should be employed as a daily function of situational awareness for all operational forces both inside and outside the classified realm.

Obviously, receipt of data does not guarantee its validity. As stated by Flt. Lt. Trevor W. M. Plant (United Kingdom), one of the most common difficulties with information is redundant and inconsistent data, as well as an unwillingness of source generators to maintain the information once generated.[12] Identifying the disparate data and resolving inconsistencies requires considerable understanding of the value of the information, its possible origins, and those who would most likely be the authority on its validity. This point is made not to restate the obvious but to emphasize that the ability to determine these factors as well as the insight to correlate seemingly unrelated pieces of information requires skill and operational understanding. It is not *solely* the realm of traditional information systems specialists.

Network Management

The need for aggressive oversight of our vastly interrelated networks cannot be overstated. Lt. Gen C. Norman Wood, USAF (Ret) best stated the situation in his August 1998 letter for *Signal* magazine:

> "Information security is likely to remain an ongoing challenge analogous to offensive versus defensive military operations. Whenever new and effective security applications are introduced, pranksters, criminals, and adversaries will immediately initiate efforts to overcome these measures. We have not yet

[11]Quote of Ked Pedersen, meeting co-chair during AFCEA's Technet 98, documented in "Network-Centric Information Potential Snags, Opportunities Become Clearer", *Signal*, Armed Forces Communications and Electronics Associations International Journal (Aug. 98), pg 83

[12]Trevor W. M. Plant, Flight Lieutenant, "Whose Information Is It Anyway? An Argument for Information Stewardship", Air Force Institute of Technology: Wright Patterson AFB, OH: Dec 1996

reached the point where our motto must be cavé datum--beware of data. However, as with any freedom, the price of liberty is eternal vigilance."[13]

The Internet has indeed become a dangerous place. Network terrorists groups have been established in countries hostile to the United States, hacker groups stage global competitions to determine who is able to penetrate the most impressive networks to the greatest extent, and protective measures taken by our communications professionals too often result in retaliatory "spamming" or flooding the network with sufficient traffic as to deny its service to the legitimate user community.

As previously mentioned, information protection organizations have been established by the services to monitor and protect the networks under their purview either at unit, theater, or DOD level (the Defense Information Systems Agency oversees the long-haul communications networks for the DOD in conjunction with Service organizations). Since this is the most well established of the proposed IMOC activities, little discussion is needed regarding the function of network monitoring. Continued emphasis must be placed on aggressive protective measures, identification of network problem areas -- whether caused by hackers or heavy network traffic -- and implementation of the latest in information technology and applications to ensure the IMOC remains at least abreast if not ahead of commercial trends.

Information Intelligence

Using the skills and knowledge of information and network management, the intelligence analysts will be able to determine what areas of the U.S. military infrastructure is being targeted by opponents. This obviously would indicate where they believe our points of

[13]C. Norman Wood, Lt Gen, USAF (Ret), "Celebrate Connectivity, But With a Caveat", *Signal*, Air Forces

vulnerability lie as well as indications of potential attack. The information intelligence analyst would serve as advisor to the traditional operational areas of air, sea, space, and land based on this gathered information. In turn, those liaison areas would work with the analyst to determine the best and appropriate means to counter enemy probes, and perhaps counter with some disinformation or probing of our own in order to shape the battlefield to our liking. The offensive use of information poses difficulties to be discussed later in this article.

Strategic Knowledge

Charles Wiseman was perhaps the first to recognize the value of information systems as strategic assets, labeling them strategic information system (SIS).[14] When properly applied in the commercial world, SIS can significantly enhance, support, and shape the competitive strategy of an organization with correspondingly improved profitability.

> "A firm with a powerful SIS vision zealously encourages the search for opportunities to use information systems to gain a competitive edge. And when they are discovered, it marshalls the proper resources to support them. In some cases, SIS vision develops into an *image* [sic] of the future that top management uses to navigate the firm's strategic path."[15]

The advantages realized by commercial business in using the information technology to its fullest extent can -- and should -- apply to military operations as well. According to V. E. Millar, information technology affects competition in three ways: 1) it changes industry structure and, in so doing, alters the rules of competition, 2) it creates competitive advantage by giving companies new ways to out-perform their rivals, and 3) it sponsors whole new

---

Communication and Electronics Association's International Journal, Aug. 1998, pg 14

[14]Charles Wiseman, *Strategy and Computers: Information Systems as Competitive Weapons*, DOW JONES-IRWIN: Homewood, IL: 1985

[15]Ibid, pg 9

businesses, often from within a company's existing operations.[16] The military corollary, of course is: 1) it requires new definition of doctrine and procedures of war, 2) it provides the U.S. military a competitive advantage over the adversary, and 3) it identifies needed technologies for future warfare.

Dr. Daniel Kuehl, in writing for the Institute for National Strategic Studies (INSS), cites Strategic Information Operations as "those military and governmental operations that protect and exploit the information environment to attain strategic objectives."[17] Artificial intelligence can significantly enhance the process of transforming raw data points into correlated data, offering potential uses of the information, and employing decision support systems to aid in expanding our strategic value of acquired knowledge. As such, it must be embedded as an integral part of the IMOC, and continued emphasis placed on expanding its capabilities. Hence, the IMOC must also support the various battle labs as they develop new weapons systems and methodologies, keeping information operations in pace with developments and responsive to the CINC's operational requirements.

Ops/Counter Ops

This is perhaps the most traditionally focused area of operation in the IMOC. Here the data gathered and validated is correlated against other known information using a blend of communications/computer skills, experience, and sleuthing necessary to produce the best product possible for fielded forces -- providing relevant, concise information when, where and how they need it.

---

[16]V. E. Millar, "How Information Gives You Competitive Advantage," *Harvard Business Review* (Jul-Aug) 1985

[17]Daniel Kuehl Dr., "Defining Information Power", *Strategic Forum No. 115,* Institute for National Strategic Studies, National Defense University (June 1997), pg 3

In addition, this is the primary area for interface with the operators and intelligence analysts to determine our critical information resources, explore our ability to exploit the weaknesses of the opponent, and development of the Information Order of Battle. Such actions may include psychological operations such as "morphing" of video clips to influence civilian population, corruption of the enemy's logistical data, or even pulsing of the enemy systems in order to render the adversary incapable of command and control of its forces.

VI. Challenges

"Policy makers and commanders in the field do not need all the information that technology affords them, because . . . beyond a certain level of information the quality of the decision product diminishes."[18]

Implementation of the organization briefly described here is not without difficulties. First, the military is only one arm providing and relying on national information power. Our ability to engage and control the information environment will rely to a great extent on the level at which we as a nation are willing to undertake similar collective action. As the military apparatus is used in an increasingly diplomatic (peacemaking, peacekeeping, or observer status) role vice actual war, the interface between purely military concerns and national objectives increases correspondingly.

Further, the ability to retain highly skilled information technologists must be recognized as significant a problem as retention of pilots, linguists, or similar highly specialized occupations. Leadership must recognize that this technology is not the realm of "geeks." It is the area of operation requiring extensive and continual training, individuals with above average intelligence, and the freedom necessary to explore all aspects of existence

[18]Goodwin, Brent Stuart, Book Review *Data Smog: Surviving the Information Glut* by David Shenk, reprinted in *Naval War College Review,* Vol. LII, Number 1, Seq 365, Winter 1999, pg 162

within the intangible, but increasingly identifiable culture of cyberspace. It is also the area of operation that affects virtually all other areas of operation before, during, and after conflict. In today's warfare environment, the CINC must have full access and control of information necessary to conduct effects based warfare either through psychological operations, network warfare, or target acquisition for modern weaponry.

Conducting operations in cyberspace requires a revisit of national and international rules of behavior. Today there is significant restrictions on offensive activities, even if taken in reaction to someone else's actions, or as a pre-emptive maneuver to secure U.S. interests. Such acts will often at least traverse the networks of other nations and may involve actions directly against another sovereignty. In the traditional world, offensive actions are considered acts of war. The INSS presents a clear picture of this difficulty:

> "... information attacks are attacks and, therefore, are subject to international law. Violations of sovereignty and acts of war are no less real because they use the information domain than if they involved violations of air space. Like other sovereign governments, the United States is free to defend itself and may choose to engage in acts of war for sufficient cause, but should not believe that this arena is an exception to normal rules of behavior. Indeed, U.S. disregard for international law in this crucial arena could set precedents that are very dangerous, in part because the United States is the world's largest potential IW [information warfare] target."[19]

The law of cyberspace, the rise of transnational social and political identification groups and the corresponding demise of sovereignty have been topics of numerable articles and debates. Reaching international consensus on where a nation's sovereign right to control it's national power -- real or information-based -- may be an impossible task. As such, an operational CINC must be aware of the political environment in which he operates and adjust

[19]"Information War and Deterrence", Institute for National Strategic Studies, National Defense University, Chap 3, pg 3

the activities of his IMOC, or indeed any information operation activities, accordingly and with full cognizance of the State Department.

VII. Conclusion

"In the next century, information technology, broadly defined, is likely to be the most important power resource."[20]

Information systems are weapons systems. They can provide discrete effects on an opponent's infrastructure or affect how he employs his military forces. They can achieve overwhelming destruction much as traditional weapons of mass destruction. The 21st Century warfighter must understand their abilities as well as their limitations, be comfortable operating in the fourth dimension of cyberspace, and prepare for battle in the electronic region just as he would in terrestrial or space conflicts. In doing so, he must remember the data carried on the systems is equally as important as the delivery system, just as the explosive device is as important as the missile body carrying it: they are integrally linked.

For the next century the United States military must undergo a change of mindset to accept this new way of war. Once achieved, the operational community, particularly at the CINC level, can organize to maximize technical capabilities, and train and execute knowledge-based warfare as needed to achieve the objectives. This refocus will in turn drive weapons systems acquisitions geared toward exploiting a commander's compressed decision cycle (a result of faster, more reliable knowledge), enabling changes to the tactical operation even as it is underway.

The theoretical organization outlined here would provide the CINC, and if deployed, the operational commander, a focused forum for knowledge acquisition and exploitation

---

[20]Keohane, pg 87

tailored to his particular region of the world. This knowledge would in turn become an important input to the national information power base where it could once again be correlated with additional sources and provide the National Command Authority a comprehensive picture of the world and events affecting our nation.

"The way of the warrior is to master the virtue of his weapons"

-- Myamoto Mushaski
The Book of Five Rings

Endnotes:

i. "During the Persian Gulf War, another communications failure, in this case an 'information glut,' threatened US and coalition operations. In Riyadh alone, over 7,000 personnel worked to put out a daily 300-page, 2,000-plus sortie air tasking order. This along with thousands of other "operationally essential" pieces of message traffic sometimes resulted in a 70,000-message backlog which meant that even the highest priority "flash" messages took four or five days to deliver." (Hutcherson, pg 31)

ii. During the peace negotiations to end fighting in the Balkans, certain Balkan leaders were reluctant to sign the Dayton Peace Accords until they were shown satellite images clearly indicating troop dispersal, etc. Knowing the U.S. could identify and intercede in any attempts at subterfuge, they acquiesced.

BIBLIOGRAPHY

Aldrich, Richard W., The International Legal Implications of Information Warfare, INSS Occasional Paper 9, Information Warfare Series, U.S. Air Force Academy: Colorado Springs, CO: USAF Institute for National Security Studies, Apr. 1996

Anonymous, "Information-age Warfare," Military Review, Vol. 78, Issue 2, Fort Leavenworth, Mar/Apr 1998, 58

Arquilla, John J. and Ronfeldt, David F., "Cyberwar is Coming", Comparative Strategy, Vol. 12, Taylor and Francis: Santa Monica, CA, 1993, 141-165.

As quoted by Megan C. Block, Capt, "AFSPC Develops Info Technology Strategy for 21st Century, Intercom , Jul. 98, 7

Berkowitz, Bruce D., "Warfare in the Information Age", Issues in Science and Technology, Fall 1995, 59-66

Casper, Lawrence E., Irving L. Halter, Earl W. Powers, Paul J. Selva, Thomas W. Stefens, and T. Lamar Willis, "Knowledged-Based Warfare: A Security Strategy for the Next Century," Joint Forces Quarterly, Ft McNair: Washington DC, Autumn 1996, 81-89

Dodge, M., "An Atlas of Cyberspace," Cyber-Geography Research, Center for Advanced Spatial Analysis, University College: London, April 7, 1999 <http://www.cybergeography.org/atlas/atlas.html>

Fitzgerald, Brian, "Jurisdiction in Cyberspace: International Issues", April 7. 1999 <http://roscoe.law.harvard.edu/courses/techseminar96/course/sessions/jurisdiction/fitzgerald.html>

Fulghum, David A., "Cyberwar Plans Trigger Intelligence Controversy," Aviation Week and Space Technology, n.p., January 19, 1998, 52 - 54

Goodwin, Brent Stuart, Book Review: "Data Smog: Surviving the Information Glut" by David Shenk, Naval War College Review, Vol. LII, Number 1, Seq 365, Winter 1999, 161-162

Hutcherson, Norman B, Lt Col. Command and Control Warfare: Putting Another Tool in the War-Fighter's Data Base, Air University Press: Maxwell AFB, AL, Sept 1994, 61

Institute for National Strategic Studies, Information War and Deterrence, National Defense University (Washington D.C.), 3

Joint Staff/J6K, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, (Washington D.C., 4 July 1995)

Keohane, Robert O. and Joseph S. Nye, Jr., "Power and Interdependence in the Information Age," Foreign Affairs, Vol. 77, No. 5, New York, NY, Sep./Oct. 1998, 81-94

Kiras, James D., "Information Warfare and the Face of Conflict in the Twenty-First Century", Peacekeeping and International Relations, Jul./Aug. 1996, 8-10

Kuehl, Daniel Dr., "Defining Information Power", Strategic Forum No. 115, Institute for National Strategic Studies, National Defense University, June 1997, 3

Libicki, Matin, "The Emerging Primacy of Information", Orbis, Vol. 40, No 2, Spring 1996, 261.

McDougal, Myres S. and Florentino P. Feliciano, The International Law of War, New Haven Press: New Haven, 1994, 872

Millar, V. E., "How Information Gives You Competitive Advantage," Harvard Business Review, Jul-Aug 1985

Murphy, Dennis M., LTC, "Information Operations on the Nontraditional Battlefield," Military Review, U.S. Army War College, Carlisle Barracks: PA, Nov-Dec 1996, 16 - 18

Office of the Secretary of Defense, Information Architecture for the Battlefield, Summer Study Task Force, Defense Science Board (Washington D.C. October 1994

Pedersen, Ked, Quote in meeting of AFCEA's Technet 98, documented in "Network-Centric Information Potential Snags, Opportunities Become Clearer", Signal, Armed Forces Communications and Electronics Associations International Journal Aug. 98, 83

Posch, Robert J., "Transactional and Attributable Nexus in Cyberspace," Direct Marketing, Vol. 59, Issue 10, Garden City: Hoke Communications, February 1997, 62-64

_____, "The Fourth-Wave--(part three)," Direct Marketing, vol. 60, Issue 12, Garden City: Hoke Communications, April 1998, 61-63

Roman, Gregory A. "The Command or Control Dilemma: When Technology and Organizational Orientation Collide," Essays on Strategy XIV, National Defense University: Washington D.C., March 1997, 149-185

Rosenbury, Laura, "A Preliminary Review of Cyber-Conflicts," April 7, 1999, <http://roscoe.law.harvard.edu/courses/techseminar96/course/sessions/jurisdiction/rosenbury.html>

Starrs, Paul F., "The Sacred, the Regional, and the Digital," Geographical Review, Vol. 87, New York: N.Y., Apr. 1997, 193-218

Plant, Trevor W. M., Flight Lieutenant, "Whose Information Is It Anyway? An Argument for Information Stewardship", Air Force Institute of Technology: Wright Patterson AFB, OH, Dec 1996

Wiseman, Charles, Strategy and Computers: Information Systems as Competitive Weapons, DOW JONES-IRWIN: Homewood, IL, 1985

Wood, C. Norman, Lt Gen, USAF (Ret), "Celebrate Connectivity, But With a Caveat", Signal, Air Forces Communication and Electronics Association's International Journal, Aug. 1998, 14